Finite Fields and Their Applications 17 (2011) 240–253

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Toward determination of optimal plane curves with a fixed degree over a finite field

Masaaki Homma [a,*,1], Seon Jeong Kim [b,2]

[a] Department of Mathematics, Kanagawa University, Yokohama 221-8686, Japan
[b] Department of Mathematics and RINS, Gyeongsang National University, Jinju 660-701, Republic of Korea

ARTICLE INFO

Article history:
Received 12 January 2010
Revised 15 September 2010
Accepted 10 December 2010
Available online 21 December 2010
Communicated by Gary McGuire

MSC:
14H50
14G15
14G05
14N10

Keywords:
Plane curve
Finite field
Rational point

ABSTRACT

For a plane curve over $\mathbb{F}_q$ of degree $q+1$, it is known by our previous work that the number of its $\mathbb{F}_q$-rational points is at most q^2+1. In this paper, we determine the curves that attain this maximum, up to projective equivalence.

1. Introduction

In the previous papers [6–8], we have studied the number of rational points of plane curves over a finite field, which was inspired by a work of Sziklai [11]. This article is also concerned with this topic. We fix a finite field $\mathbb{F}_q$ of q elements, and the projective plane $\mathbb{P}^2$ over $\mathbb{F}_q$. The set of $\mathbb{F}_q$-points of $\mathbb{P}^2$ is denoted by $\mathbb{P}^2(\mathbb{F}_q)$, and for a plane curve C, $C(\mathbb{F}_q)$ means $C \cap \mathbb{P}^2(\mathbb{F}_q)$. Our curve C may be reducible, but C has no $\mathbb{F}_q$-linear components. The cardinality of $C(\mathbb{F}_q)$ is denoted by $N_q(C)$.

* Corresponding author.
E-mail addresses: homma@kanagawa-u.ac.jp (M. Homma), skim@gnu.kr (S.J. Kim).

[1] Partially supported by Grant-in-Aid for Scientific Research (21540051), JSPS.
[2] Partially supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2009-0088321).

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2010.12.003

What we proved mainly in the previous papers is the following theorem.

Theorem 1.1. *Under the above hypotheses and notation, if the degree of C is d, then*

$$N_q(C) \leqslant (d-1)q + 1 \tag{1}$$

except for the curve over $\mathbb{F}_4$ defined by

$$X^4 + Y^4 + Z^4 + X^2Y^2 + Y^2Z^2 + Z^2X^2 + X^2YZ + XY^2Z + XYZ^2 = 0.$$

The bound (1) was originally conjectured in [11] mentioned above, so we refer to this bound as Sziklai's upper bound.

Now we explain our program of further research after established Theorem 1.1. We introduce more notation. Let $\mathcal{C}_d(\mathbb{F}_q)$ be the set of plane curves of degree d over $\mathbb{F}_q$ without $\mathbb{F}_q$-linear components, $\mathcal{C}_d^i(\mathbb{F}_q)$ the subset of $\mathcal{C}_d(\mathbb{F}_q)$ whose members are irreducible, and $\mathcal{C}_d^s(\mathbb{F}_q)$ nonsingular. We consider three numbers for a fixed degree d:

(i) $M_q(d) = \max\{N_q(C) \mid C \in \mathcal{C}_d(\mathbb{F}_q)\}$;
(ii) $M_q^i(d) = \max\{N_q(C) \mid C \in \mathcal{C}_d^i(\mathbb{F}_q)\}$;
(iii) $M_q^s(d) = \max\{N_q(C) \mid C \in \mathcal{C}_d^s(\mathbb{F}_q)\}$.

One of the further targets is to determine those numbers exactly. Obviously $M_q(d) \geqslant M_q^i(d) \geqslant M_q^s(d)$ holds. These inequalities can possibly be strict, which are explained by examples in Appendix A.

We already know the exact value of $M_q(d)$ for some cases:

(A) If $d \geqslant q+3$, then $M_q(d) = q^2 + q + 1$ [6, Prop. 1.1];
(B) If $d = q+2$, then $M_q(q+2) = M_q^i(q+2) = M_q^s(q+2) = q^2 + q + 1$ [12,5];
(C) If $d = q+1$, then $M_q(q+1) = M_q^i(q+1) = M_q^s(q+1) = q^2 + 1$ [6];
(D) If $d = q \neq 4$, then $M_q(q) = M_q^i(q) = M_q^s(q) = q^2 - q + 1$ [7]; and $M_4(4) = M_4^i(4) = M_4^s(4) = 14$ if $d = q = 4$ [10];
(E) If $d = q-1$, then $M_q(q-1) = M_q^i(q-1) = M_q^s(q-1) = q^2 - 2q + 1$ [11].

Here are some remarks. The value $q^2 + q + 1$ appeared in (A) and (B) is just the number of $\mathbb{F}_q$-points of $\mathbb{P}^2$, and each value appeared in (B), (C), (D) or (E) agrees with Sziklai's upper bound. The reference at the end of each item in the list shows a source of an example which attains the trivial upper bound $q^2 + q + 1$ or Sziklai's.

The following fact is also worth pointing out.

Remark 1.2. Suppose $M_q(d)$ agrees with Sziklai's upper bound $(d-1)q + 1$. Then, for each curve $C \in \mathcal{C}_d(\mathbb{F}_q)$ with $N_q(C) = M_q(d)$, C is absolutely irreducible and any $\mathbb{F}_q$-point of C is nonsingular. One can find its proof in [7, Section 2].

After we know the exact value of $M_q(d)$, it must be interesting to classify or to determine all curves that attain $M_q(d)$. In this paper, we take a step toward this problem, and handle the case $d = q+1$. Note that the classification for $d = q+2$ is already done by Tallini [12] (see also [5]) from another interest.

An example of a curve of degree $q+1$ over $\mathbb{F}_q$ with q^2+1 rational points is the curve defined by

$$X^{q+1} - X^2Z^{q-1} + Y^qZ - YZ^q = 0, \tag{2}$$

which is nonsingular. The purpose of this paper is to prove the following theorem.

Theorem 1.3. *Let $C \in \mathcal{C}_{q+1}(\mathbb{F}_q)$ with $N_q(C) = q^2 + 1$.*

(i) *If $q \geqslant 5$ or $q = 2$, then C is projectively equivalent to the curve* (2) *over $\mathbb{F}_q$.*
(ii) *If $q = 4$, then C is projectively equivalent over $\mathbb{F}_4$ to either* (2) *or the curve*

$$\eta\big(X^4Y + XY^4 + Y^4Z + YZ^4 + Z^4X + ZX^4\big) + XYZ\big(\eta^2\big(X^2 + Y^2 + Z^2\big) + XY + YZ + ZX\big) = 0, \tag{3}$$

where $\eta \in \mathbb{F}_4$ satisfies the equation $\eta^2 + \eta + 1 = 0$. Those two curves (2) *and* (3) *are not projectively equivalent over $\mathbb{F}_4$ each other.*
(iii) *If $q = 3$, then C is projectively equivalent over $\mathbb{F}_3$ to either* (2) *or the curve*

$$X^3Y - XY^3 + Y^3Z - YZ^3 + Z^3X - ZX^3 + XYZ(X + Y - Z) = 0. \tag{4}$$

Those two curves (2) *and* (4) *are not projectively equivalent over $\mathbb{F}_3$ each other.*

Notation. The projective space of lines of $\mathbb{P}^2$ is denoted by $\check{\mathbb{P}}^2$. We understand the coordinates U, V, W of $\check{\mathbb{P}}^2$ are determined by those X, Y, Z of $\mathbb{P}^2$ with the relation $UX + VY + WZ = 0$. So $\check{\mathbb{P}}^2(\mathbb{F}_q)$ means the set of $\mathbb{F}_q$-lines of $\mathbb{P}^2$. For an $\mathbb{F}_q$-point $P \in \mathbb{P}^2$, $\check{P}$ denotes the set $\{l \in \check{\mathbb{P}}^2(\mathbb{F}_q) \mid l \ni P\}$. Occasionally, we use $\check{l}$ for the point of $\check{\mathbb{P}}^2(\mathbb{F}_q)$ corresponding with an $\mathbb{F}_q$-line l.

For two points $P, Q \in \mathbb{P}^2(\mathbb{F}_q)$, PQ denotes the line passing through P and Q.

We frequently use the notation like $\{F = 0\}$ which stands for "the curve defined by equation $F = 0$".

When we fix a curve C over $\mathbb{F}_q$, for an integer i,

$$\mathcal{A}_i = \big\{l \in \check{\mathbb{P}}^2(\mathbb{F}_q) \;\big|\; {}^{\#}\big(l(\mathbb{F}_q) \cap C\big) = i\big\},$$

where $^{\#}$ stands for "the number of".

2. Some observations and the case $q \geqslant 5$ or $q = 2$

Let $C \in \mathcal{C}_{q+1}(\mathbb{F}_q)$ with $N_q(C) = q^2 + 1$. Then C is absolutely irreducible without $\mathbb{F}_q$-rational singular points, as was mentioned in Introduction. Let $Z(C) = \mathbb{P}^2(\mathbb{F}_q) \setminus C$. If the q points of $Z(C)$ are collinear, then C is projectively equivalent to the curve (2) [6, Prop. 2.4]. Actually, if $q \geqslant 5$, then the q points of $Z(C)$ are collinear, which is what we show first. After finishing the proof, we will observe the case where the q points of $Z(C)$ are not collinear.

Theorem 2.1. *Let $C \in \mathcal{C}_{q+1}(\mathbb{F}_q)$ with $N_q(C) = q^2 + 1$. Suppose $q \geqslant 5$ or $q = 2$. Then C is projectively equivalent to the curve*

$$X^{q+1} - X^2Z^{q-1} + Y^qZ - YZ^q = 0,$$

and hence, nonsingular.

Proof. As was explained above, it is enough to show that the q points of $Z(C)$ are collinear. When $q = 2$, this holds trivially. So we suppose $q \geqslant 5$. Recall $\mathcal{A}_{q+1} = \{l \in \check{\mathbb{P}}^2(\mathbb{F}_q) \mid {}^{\#}(l \cap C(\mathbb{F}_q)) = q + 1\}$.

The first claim is that there are three lines in $\mathcal{A}_{q+1}$ that are concurrent. Choose a point $P_0 \in C(\mathbb{F}_q)$, and consider the partition $\mathbb{P}^2(\mathbb{F}_q) \setminus \{P_0\} = \coprod_{l \in \check{P}_0} (l(\mathbb{F}_q) \setminus \{P_0\})$. Since ${}^{\#}Z(C) = q$, there is at least a line $l_1 \in \check{P}_0 \cap \mathcal{A}_{q+1}$. Fix this line l_1, and consider the correspondence

$$\mathcal{T} = \left\{ \left(\left\{ Q, Q' \right\}, P \right) \in \left(S^2 Z(C) \setminus \Delta \right) \times l_1(\mathbb{F}_q) \;\middle|\; Q\,Q' \ni P \right\}$$

with two projections $\pi_1 : \mathcal{T} \to S^2 Z(C) \setminus \Delta$ and $\pi_2 : \mathcal{T} \to l_1(\mathbb{F}_q)$, where $S^2 Z(C)$ is the symmetric product of two copies of $Z(C)$ and Δ is the diagonal set. Since π_1 is bijective, ${}^{\#}\mathcal{T} = \binom{q}{2}$. Since ${}^{\#}l_1(\mathbb{F}_q) = q+1$ and $q \geqslant 5$, there is a point $P_1 \in l_1(\mathbb{F}_q)$ such that ${}^{\#}\pi_2^{-1}(P_1) \geqslant 2$. This means that either there are two lines $m_1, m_2 \in \check{P}_1$ such that ${}^{\#}(m_i \cap Z(C)) \geqslant 2$ $(i = 1, 2)$, or there is a line $m \in \check{P}_1$ such that ${}^{\#}(m \cap Z(C)) \geqslant 3$. Counting the number of points in $Z(C)$ by using the partition $\mathbb{P}^2(\mathbb{F}_q) \setminus \{P_1\} = \coprod_{l \in \check{P}_1} (l(\mathbb{F}_q) \setminus \{P_1\})$, we know there are two lines $l_2, l_3 \in (\check{P}_1 \setminus \{l_1\}) \cap \mathcal{A}_{q+1}$ because ${}^{\#}(\check{P}_1 \setminus \{l_1, m_1, m_2\}) - ({}^{\#}Z(C) - 4) \geqslant 2$ in the former case, and ${}^{\#}(\check{P}_1 \setminus \{l_1, m\}) - ({}^{\#}Z(C) - 3) \geqslant 2$ in the latter case. Those three lines l_1, l_2 and l_3 have the required property.

Next we choose coordinates X, Y, Z as $P_1 = (0, 0, 1)$. Let $k = {}^{\#}(\check{P}_1 \cap \mathcal{A}_{q+1})$ and $\check{P}_1 \cap \mathcal{A}_{q+1} = \{l_1, \ldots, l_k\}$. By the choice of P_1, $k \geqslant 3$, and by the fact $C(\mathbb{F}_q) \neq \mathbb{P}^2(\mathbb{F}_q)$, $k \leqslant q$. Write an equation of C as

$$F(X, Y, Z) = g_{q+1}(X, Y) + g_q(X, Y)Z + \cdots + g_1(X, Y)Z^q + g_0 Z^{q+1} = 0,$$

where $g_j(X, Y)$ is a homogeneous polynomial of degree j. Note that $g_0 = 0$ because $F(0, 0, 1) = 0$. Since $\lambda^q = \lambda$ for any $\lambda \in \mathbb{F}_q$, $C(\mathbb{F}_q)$ coincides with the $\mathbb{F}_q$-solutions of the homogeneous equation

$$\tilde{g}_{q+1}(X, Y) + \tilde{g}_q(X, Y)Z + \cdots + \tilde{g}_2(X, Y)Z^{q-1} = 0,$$

where

$$\tilde{g}_s(X, Y) = \begin{cases} g_s(X, Y) & (s = 2, \ldots, q-1, q+1), \\ g_q(X, Y) + g_1(X^q, Y^q) & (s = q). \end{cases}$$

For each $l_i \in \check{P}_1 \cap \mathcal{A}_{q+1}$, we can write as

$$l_i(\mathbb{F}_q) = \left\{ (\alpha_i, \beta_i, \lambda) \;\middle|\; \lambda \in \mathbb{F}_q \right\} \cup \left\{ (0, 0, 1) \right\}$$

for a suitable $(\alpha_i, \beta_i) \in \mathbb{P}^1(\mathbb{F}_q)$. Choose a primitive element γ of $\mathbb{F}_q$. Since $l_i(\mathbb{F}_q) \subset C$, we have

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 1 & 1 & \cdots & 1 \\ 1 & \gamma & \cdots & \gamma^{q-1} \\ \vdots & \vdots & & \vdots \\ 1 & \gamma^{q-2} & \cdots & (\gamma^{q-2})^{q-1} \end{pmatrix} \begin{pmatrix} \tilde{g}_{q+1}(\alpha_i, \beta_i) \\ \tilde{g}_q(\alpha_i, \beta_i) \\ \tilde{g}_{q-1}(\alpha_i, \beta_i) \\ \tilde{g}_{q-2}(\alpha_i, \beta_i) \\ \vdots \\ \tilde{g}_2(\alpha_i, \beta_i) \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Since the determinant of the q by q matrix is nonzero, we have $\tilde{g}_s(\alpha_i, \beta_i) = 0$ $(s = 2, \ldots, q+1)$. Since $\tilde{g}_s(X, Y) = 0$ has k solutions $\{(\alpha_i, \beta_i)\}_{1 \leqslant i \leqslant k}$ and is of degree s, $\tilde{g}_s(X, Y) = 0$ as polynomials for $s = 2, \ldots, k-1$. Therefore $C(\mathbb{F}_q)$ coincides with the $\mathbb{F}_q$-solutions of the equation $\sum_{s=k}^{q+1} \tilde{g}_s(X, Y)Z^{q+1-s} = 0$. For other line $m \in \check{P}_1 \setminus \mathcal{A}_{q+1}$, ${}^{\#}(m \cap C(\mathbb{F}_q)) \leqslant q + 2 - k$. In fact, write $m(\mathbb{F}_q) = \{(\alpha, \beta, \lambda) \mid \lambda \in \mathbb{F}_q\} \cup \{(0, 0, 1)\}$. Then ${}^{\#}(m \cap C(\mathbb{F}_q))$ is equal to the number of solutions in $\mathbb{F}_q$ of

$$\sum_{s=k}^{q+1} \tilde{g}_s(\alpha, \beta) Z^{q+1-s} = 0 \tag{5}$$

plus 1. If $^{\#}(m \cap C(\mathbb{F}_q)) > q+2-k$, then Eq. (5) must be trivial, so $m(\mathbb{F}_q) \subset C$, which is contradictory to the minimality of k. Hence

$$q = {}^{\#}Z(C) = \sum_{m \in \check{P}_1 \setminus \mathcal{A}_{q+1}} m \cap Z(C) \geqslant {}^{\#}(\check{P}_1 \setminus \mathcal{A}_{q+1}) \cdot (k-1) = (q+1-k)(k-1).$$

Hence $(q-k)(2-k)+1 \geqslant 0$. Since $k \geqslant 3$ and $q \geqslant 5$, we have $k \geqslant q$. Actually if $k \geqslant 4$, it is obvious; and if $k = 3$, the inequality implies $q \leqslant 4$. Therefore $k = q$, so $Z(C)$ is contained in a line. □

Corollary 2.2. *A curve $C \in \mathcal{C}_{q+1}(\mathbb{F}_q)$ with $N_q(C) = q^2+1$ is nonsingular.*

Proof. When $q \geqslant 5$ or $q = 2$, this follows from Theorem 2.1. Only remaining cases are $q = 3$ and 4. Since $N_q(C)$ agrees with Sziklai's upper bound, C is absolutely irreducible and any $\mathbb{F}_q$-point of C is nonsingular by Remark 1.2. Let $\tilde{C} \to C$ be the normalization of C. Then $\tilde{C}$ is also defined over $\mathbb{F}_q$ and $\tilde{C}(\mathbb{F}_q) \to C(\mathbb{F}_q)$ is bijective.

If $q = 4$ and C has singularities, then the genus of $\tilde{C}$ is at most 4. In fact, since any singular point of C is not $\mathbb{F}_q$-rational, its conjugate over $\mathbb{F}_q$ is also singular. Hence the genus of $\tilde{C}$ is at most $\frac{1}{2}(5-1)(5-2)-2 = 4$. The list of maximum number of $\mathbb{F}_4$-rational points of a nonsingular curve of genus at most 4 is as follows [1]:

genus	0	1	2	3	4
max. num. of $\mathbb{F}_4$-pts.	5	9	10	14	15

Since $N_4(C) = 17$, C can't have singularities.

For the case $q = 3$, similar argument works well, that is, the genus of the normalization of C is at most 1 if C has singularities, and the corresponding list is:

genus	0	1
max. num. of $\mathbb{F}_3$-pts.	4	7

but $N_3(C) = 10$. □

In the rest of this section, we prepare for the study of the case where the q points of $Z(C)$ are not collinear. By this condition, $q \geqslant 3$ a priori.

Lemma 2.3. *Let $C \in \mathcal{C}_{q+1}(\mathbb{F}_q)$ with $N_q(C) = q^2+1$. If the q points of $Z(C)$ are not collinear, then, after changing coordinates, C is defined by the following type of equation*:

$$a\big(X^qY - XY^q\big) + b\big(Y^qZ - YZ^q\big) + c\big(Z^qX - ZX^q\big) + XYZh(X,Y,Z) = 0, \tag{6}$$

where $a, b, c \in \mathbb{F}_q^\times$ and $h(X,Y,Z)$ is a homogeneous polynomial of degree $q-2$ over $\mathbb{F}_q$.

Proof. The first claim is that there are non-concurrent three lines in $\mathcal{A}_{q+1}$. Choose three points $Q_1, Q_2, Q_3 \in Z(C)$ so that they are not collinear, and $P_1 \in Q_1Q_2 \cap C(\mathbb{F}_q)$. Since $^{\#}(Z(C) \setminus \{Q_1, Q_2\}) = q-2$, there are at least two lines $l_1, l_2 \in \check{P}_1 \cap \mathcal{A}_{q+1}$. Let $P_2 = l_2 \cap Q_2Q_3$, which can't be P_1. By the same reason as above, two lines in $\check{P}_2 \cap \mathcal{A}_{q+1}$ will be found out, one of which may be l_2. Choose $l_3 \in \check{P}_2 \cap \mathcal{A}_{q+1}$ which is different from l_2. Then these three lines l_1, l_2, l_3 have the required property.

Next we choose coordinates X, Y, Z as $l_1 = \{X = 0\}$, $l_2 = \{Y = 0\}$, $l_3 = \{Z = 0\}$, and an equation $F(X,Y,Z) = 0$ of C. Since $F(X,Y,0) =$ for any $(X,Y) \in \mathbb{P}^1(\mathbb{F}_q) = l_3(\mathbb{F}_q)$ and the degree of F is

$q+1$, $F(X,Y,Z) = a(X^qY - XY^q) \bmod Z$. Hence $F(X,Y,Z) = a(X^qY - XY^q) + Zf_1(X,Y,Z)$, where $f_1(X,Y,Z)$ is a homogeneous polynomial of degree q. Considering $Zf_1(0,Y,Z) = F(0,Y,Z) = 0$ for any $(Y,Z) \in \mathbb{P}^1(\mathbb{F}_q) = l_1(\mathbb{F}_q)$, we have $Zf_1(X,Y,Z) = b(Y^qZ - YZ^q) + XZf_2(X,Y,Z)$, where $f_2(X,Y,Z)$ is a homogeneous polynomial of degree $q-1$. Repeating the procedure, we have the desired form of F. Note that in Eq. (6), a, b, c are nonzero, because X or Y or Z divides F if b or c or a is 0 respectively. □

Remark 2.4. Since the first three terms of Eq. (6) vanish on the $\mathbb{P}^2(\mathbb{F}_q)$,

$$C(\mathbb{F}_q) = l_1(\mathbb{F}_q) \cup l_2(\mathbb{F}_q) \cup l_3(\mathbb{F}_q) \cup H(\mathbb{F}_q),$$

where $H = \{h = 0\}$. This is true, even if the curve defined by (6) has $\mathbb{F}_q$-linear components.

3. The case $q = 3$

The target of this section is to show the following theorem.

Theorem 3.1. *There is a unique plane curve C over $\mathbb{F}_3$ of degree 4 without $\mathbb{F}_3$-linear components, up to projective linear transformation over $\mathbb{F}_3$, such that*

(i) $C(\mathbb{F}_3) = 10$;
(ii) *the three points of $Z(C)$ are not collinear.*

Moreover, under a suitable choice of coordinates, the curve is defined by (4).

By Lemma 2.3, we already know a curve with properties (i), (ii) above is projectively equivalent to a curve with a defining equation of type

$$a\big(X^3Y - XY^3\big) + b\big(Y^3Z - YZ^3\big) + c\big(Z^3X - ZX^3\big) + XYZ(\alpha X + \beta Y + \gamma Z) = 0. \tag{7}$$

Let $C(a,b,c;\alpha,\beta,\gamma)$ denote the curve (7), and l_1, l_2, l_3 and l_4 be lines $\{X=0\}$, $\{Y=0\}$, $\{Z=0\}$ and $\{\alpha X + \beta Y + \gamma Z = 0\}$ respectively. For a moment, $C(a,b,c;\alpha,\beta,\gamma)$ is allowed to have $\mathbb{F}_3$-linear components.

Lemma 3.2. *Let $D = C(a,b,c;\alpha,\beta,\gamma)$ which may have $\mathbb{F}_3$-linear components. Then $N_q(D) = 10$ if and only if no three of the four lines l_1, l_2, l_3, l_4 are concurrent, which is also equivalent to the condition $\alpha\beta\gamma \neq 0$.*

Proof. As was mentioned in Remark 2.4, $D(\mathbb{F}_3) = \bigcup_{i=1}^4 l_i(\mathbb{F}_3)$.

It is not hard to see the following fact: for four $\mathbb{F}_3$-lines m_1, m_2, m_3, m_4 of $\mathbb{P}^2$,

(i) if no three of them are concurrent, then $^{\#}(\bigcup_{i=1}^4 m_i(\mathbb{F}_3)) = 10$;
(ii) if some three lines are concurrent, but other triple of lines are not, then $^{\#}(\bigcup_{i=1}^4 m_i(\mathbb{F}_3)) = 11$;
(iii) if the four lines are concurrent, then $^{\#}(\bigcup_{i=1}^4 m_i(\mathbb{F}_3)) = 13$.

It is obvious that no three of the four vectors $(1,0,0)$, $(0,1,0)$, $(0,0,1)$, (α,β,γ) are linearly dependent if and only if $\alpha\beta\gamma \neq 0$. □

Lemma 3.3. *Let $D = C(a,b,c;\alpha,\beta,\gamma)$ with $N_3(D) = 10$. Then possible $\mathbb{F}_3$-linear components of D are l_1, l_2, l_3 and l_4.*

Proof. Let l be an $\mathbb{F}_3$-line other than the l_i's. If no three of the five lines $l_1, \dots, l_4$ and l are concurrent, the five points $\check{l}_1, \dots, \check{l}_4, \check{l} \in \check{\mathbb{P}}^2(\mathbb{F}_3)$ form an arc, which is impossible because over $\mathbb{F}_3$ [3, Th. 8.5]. Hence some two lines of $l_1, \dots, l_4$ and l are concurrent by Lemma 3.2. Therefore

$$\#\big(l \cap D(\mathbb{F}_3)\big) = \#\left(l \cap \left(\bigcup_{i=1}^{4} l_i(\mathbb{F}_3)\right)\right) = \#\left(\bigcup_{i=1}^{4} \big(l \cap l_i(\mathbb{F}_3)\big)\right) \leqslant 3$$

because some two points of $\{l \cap l_i(\mathbb{F}_3)\}_i$ are the same, which implies that l is not a component of D. □

Lemma 3.4. *The curve defined by*

$$a\big(X^3Y - XY^3\big) + b\big(Y^3Z - YZ^3\big) + c\big(Z^3X - ZX^3\big) = 0$$

with $a, b, c \in \mathbb{F}_3$ is the union of four $\mathbb{F}_3$-lines passing through $(b, c, a) \in \mathbb{P}^2(\mathbb{F}_3)$.

Proof. See [5, Prop. 2.3]. □

Corollary 3.5. *l_1, l_2, l_3 or l_4 is a component of $D = C(a, b, c; \alpha, \beta, \gamma)$ if and only if $b = 0$, $c = 0$, $a = 0$ or $\alpha b + \beta c + \gamma a = 0$ respectively.*

Proof. Because D is defined by (7), l_i is a component of D if and only if it is a component of the curve

$$a\big(X^3Y - XY^3\big) + b\big(Y^3Z - YZ^3\big) + c\big(Z^3X - ZX^3\big) = 0,$$

which means that $l_i \ni (b, c, a)$ by Lemma 3.4. □

Proof of Theorem 3.1. From Lemma 3.2 and Corollary 3.5, C is projectively equivalent to one of the curves

$$\mathcal{C}' = \big\{C(a, b, c; \alpha, \beta, \gamma) \;\big|\; \alpha\beta\gamma \neq 0,\ abc \neq 0,\ \alpha b + \beta c + \gamma a \neq 0\big\},$$

and any member of $\mathcal{C}'$ has the required properties.

Since no three of $l_1, \dots, l_4$ are concurrent, there exists $\sigma \in PGL(3, \mathbb{F}_3)$ such that $\sigma(\{l_1, \dots, l_4\}) = \{l_1, l_2, l_3, \{X + Y - Z = 0\}\}$, which means that any member of $\mathcal{C}'$ is projectively equivalent to a curve in the subfamily

$$\mathcal{C}'' = \big\{C(a, b, c; 1, 1, -1) \;\big|\; abc(b + c - a) \neq 0\big\}.$$

The subfamily $\mathcal{C}''$ consists of six members, namely $C(a, b, c; 1, 1, -1) \in \mathcal{C}''$ if and only if $(a, b, c) \in (\mathbb{F}_3^{\times})^3 \setminus \{(1, -1, -1), (-1, 1, 1)\}$. Now we consider two projectivities $\sigma_0, \tau_0 \in PGL(3, \mathbb{F}_3)$ defined by $\sigma_0(X) = Y$, $\sigma_0(Y) = X$, $\sigma_0(Z) = Z$ and $\tau_0(X) = X + Y - Z$, $\tau_0(Y) = -Y$, $\tau_0(Z) = -Z$ respectively. Then

$$\sigma_0\big(C(a, b, c; 1, 1, -1)\big) = C(-a, -c, -b; 1, 1, -1),$$
$$\tau_0\big(C(a, b, c; 1, 1, -1)\big) = C(-a, b + c - a, -c; 1, 1, -1).$$

Hence the group generated by σ_0 and τ_0 acts on $\mathcal{C}''$ transitively, because

$$\begin{aligned} C(1,1,1;1,1,-1) &\overset{\tau_0}{\mapsto} C(-1,1,-1;1,1,-1) \\ &\overset{\sigma_0}{\mapsto} C(1,1,-1;1,1,-1) \\ &\overset{\tau_0}{\mapsto} C(-1,-1,1;1,1,-1) \\ &\overset{\sigma_0}{\mapsto} C(1,-1,1;1,1,-1) \\ &\overset{\tau_0}{\mapsto} C(-1,-1,-1;1,1,-1). \end{aligned}$$

The equation of $C(1,1,1;1,1,-1)$ is the desired one. □

4. The case $q = 4$

In this section, we work over $\mathbb{F}_4 = \mathbb{F}_2[\eta]$, where η is a primitive third root of 1, that is, $\eta^2 + \eta + 1 = 0$.

Theorem 4.1. *There is a unique plane curve C over $\mathbb{F}_4$ of degree 5 without $\mathbb{F}_4$-linear components, up to projective linear transformation over $\mathbb{F}_4$, such that*

(i) $C(\mathbb{F}_4) = 17$;
(ii) *the four points of $Z(C)$ are not collinear.*

Moreover, under a suitable choice of coordinates, the curve is defined by (3).

Before the proof of this theorem, we investigate the curve C_0 defined by (3). For simplicity, $h_0(X,Y,Z)$ denotes $\eta^2(X^2+Y^2+Z^2) + XY + YZ + ZX$, and $H_0 = \{h_0 = 0\}$. As was mentioned in Remark 2.4, $C_0(\mathbb{F}_4) = (\bigcup_{i=1}^{3} l_i(\mathbb{F}_4)) \cup H_0(\mathbb{F}_4)$, where $l_1 = \{X = 0\}$, $l_2 = \{Y = 0\}$, $l_3 = \{Z = 0\}$.

Lemma 4.2. *$l_i \cap H_0$ has no $\mathbb{F}_4$-rational points for $i = 1, 2, 3$.*

By the symmetry of h_0 in X, Y, Z, it is enough to see for $l_1 = \{X = 0\}$. It is easy to see that $(0, \beta, \gamma) \in H_0$ if and only if $(\frac{\beta}{\gamma})^2 + \eta(\frac{\beta}{\gamma}) + 1 = 0$. Hence $\frac{\beta}{\gamma} \notin \mathbb{F}_4$.

By this lemma,

$$N_4(C_0) = {}^{\#}\left(\bigcup_{i=1}^{3} l_i(\mathbb{F}_4)\right) + {}^{\#}H_0(\mathbb{F}_4) = 4 \times 3 + 5 = 17,$$

and hence C_0 is a curve of $\mathcal{C}_5(\mathbb{F}_4)$ that attains Sziklai's upper bound if C_0 has no $\mathbb{F}_4$-linear components. Nonexistence of any $\mathbb{F}_4$-linear components of C_0 will be proved in Proposition 4.6 later.

Lemma 4.3. $Z(C_0) = \{(1,1,1), (\eta,1,1), (1,\eta,1), (1,1,\eta)\}$.

Proof. Since $h(1,1,1) = \eta^2 + 1$ and $h(\eta,1,1) = h(1,\eta,1) = h(1,1,\eta) = \eta + 1$, these four points are in $Z(C_0)$. Since $N_4(C_0) = 17$, ${}^{\#}Z(C_0) = 4$. □

Let $m_0 = \{X + Y + Z = 0\}$, $m_1 = \{\eta X + Y + Z = 0\}$, $m_2 = \{X + \eta Y + Z = 0\}$, $m_3 = \{X + Y + \eta Z = 0\}$.

Lemma 4.4. *For a line $l \in \check{\mathbb{P}}^2(\mathbb{F}_4)$, $l(\mathbb{F}_4) \subset C_0$ if and only if l is one of the seven lines $l_1, l_2, l_3, m_0, m_1, m_2, m_3$.*

Proof. For a given $\mathbb{F}_4$-line l with equation $aX+bY+cZ=0$, we understand the coordinates of $\check{l}\in\check{\mathbb{P}}^2$ as (a,b,c). Since $l(\mathbb{F}_4)\subset C_0(\mathbb{F}_4)$ if and only if $l\cap Z(C_0)=\emptyset$, the set of $\mathbb{F}_4$-lines with this property is

$$\left\{(a,b,c)\in\check{\mathbb{P}}^2(\mathbb{F}_4)\;\middle|\;\begin{array}{c}a+b+c\neq 0\\ \eta a+b+c\neq 0\\ a+\eta b+c\neq 0\\ a+b+\eta c\neq 0\end{array}\right\}. \tag{8}$$

The cardinality of the set (8) is

$$\#\check{\mathbb{P}}^2(\mathbb{F}_4)-\#\left\{l\in\check{\mathbb{P}}^2(\mathbb{F}_4)\;\middle|\;l\cap Z(C_0)\neq\emptyset\right\}=21-\left(5\times 4-\binom{4}{2}\right)=7,$$

because no three points of $Z(C_0)$ are collinear. Obviously $(1,0,0)$, $(0,1,0)$ and $(0,0,1)$ are members of the set (8). The remaining four members of (8) are $(1,1,1)$, $(\eta,1,1)$, $(1,\eta,1)$ and $(1,1,\eta)$. □

The computations hereafter are rather complicate. In order to make those clearer, we prepare auxiliary calculation.

Lemma 4.5. *Let $u_{ij}\in\mathbb{F}_4$ for $i=1,2,3$; $j=X,Y,Z$. If*

$$\begin{pmatrix}X'\\Y'\\Z'\end{pmatrix}=\begin{pmatrix}u_{1X}&u_{1Y}&u_{1Z}\\u_{2X}&u_{2Y}&u_{2Z}\\u_{3X}&u_{3Y}&u_{3Z}\end{pmatrix}\begin{pmatrix}X\\Y\\Z\end{pmatrix},$$

then

$$\begin{pmatrix}X'^4Y'+X'Y'^4\\Y'^4Z'+Y'Z'^4\\Z'^4X'+Z'X'^4\end{pmatrix}=\begin{pmatrix}\begin{vmatrix}u_{1X}&u_{1Y}\\u_{2X}&u_{2Y}\end{vmatrix}&\begin{vmatrix}u_{1Y}&u_{1Z}\\u_{2Y}&u_{2Z}\end{vmatrix}&\begin{vmatrix}u_{1Z}&u_{1X}\\u_{2Z}&u_{2X}\end{vmatrix}\\ \begin{vmatrix}u_{2X}&u_{2Y}\\u_{3X}&u_{3Y}\end{vmatrix}&\begin{vmatrix}u_{2Y}&u_{2Z}\\u_{3Y}&u_{3Z}\end{vmatrix}&\begin{vmatrix}u_{2Z}&u_{2X}\\u_{3Z}&u_{3X}\end{vmatrix}\\ \begin{vmatrix}u_{3X}&u_{3Y}\\u_{1X}&u_{1Y}\end{vmatrix}&\begin{vmatrix}u_{3Y}&u_{3Z}\\u_{1Y}&u_{1Z}\end{vmatrix}&\begin{vmatrix}u_{3Z}&u_{3X}\\u_{1Z}&u_{1X}\end{vmatrix}\end{pmatrix}\begin{pmatrix}X^4Y+XY^4\\Y^4Z+YZ^4\\Z^4X+ZX^4\end{pmatrix}.$$

Proof. This is a particular case of [5, Lem. 2.2], but one can check this formula by straightforward computation. □

We introduce further curves. Let $a,b,c\in\mathbb{F}_4$ and

$$F_{(a,b,c)}(X,Y,Z)=a\big(X^4Y+XY^4\big)+b\big(Y^4Z+YZ^4\big)+c\big(Z^4X+ZX^4\big)+XYZh_0(X,Y,Z).$$

$C_{(a,b,c)}$ denotes the curve $\{F_{(a,b,c)}(X,Y,Z)=0\}$. Note that $C_{(\eta,\eta,\eta)}=C_0$ and $C_{(a,b,c)}(\mathbb{F}_4)=C_0(\mathbb{F}_4)$ by Remark 2.4. Hence Lemmas 4.3 and 4.4 are true for $C_{(a,b,c)}$ instead of for C_0.

Proposition 4.6. *$C_{(a,b,c)}$ does not contain any $\mathbb{F}_4$-line as a component if and only if (a,b,c) is either (η,η,η) or (η,η^2,η^2) or (η^2,η,η^2) or (η^2,η^2,η). Moreover these four curves are nonsingular.*

Proof. By Lemma 4.4 with the above note, the possibilities of $\mathbb{F}_4$-linear component of $C_{(a,b,c)}$ are the seven lines $l_1,\dots,m_3$. It is easy to see that l_1 or l_2 or l_3 is a component of $C_{(a,b,c)}$ if and only if $b=0$ or $c=0$ or $a=0$ respectively. For $m_0,\dots,m_3$, we can choose their equations as $Z=uX+vY$, where

$$(u,v)=\begin{cases}(1,1) & \text{for } m_0,\\ (\eta,1) & \text{for } m_1,\\ (1,\eta) & \text{for } m_2,\\ (\eta^2,\eta^2) & \text{for } m_3.\end{cases}$$

We want to observe $F_{(a,b,c)}(X,Y,uX+vY)$. To the first three terms, Lemma 4.5 is applicable. Namely, if $X'=X$, $Y'=Y$, $Z'=uX+vY$, then

$$a\big(X^4Y+XY^4\big)+b\big(Y^4Z'+YZ'^4\big)+c\big(Z'^4X+Z'X^4\big)=(a+bu+cv)\big(X^4Y+XY^4\big).$$

For the last term,

$$\begin{aligned}&XYZ'\big(\eta^2\big(X^2+Y^2+Z'^2\big)+XY+YZ'+Z'X\big)\\ &\quad=u\big(\eta^2+\eta^2u^2+u\big)X^4Y+v\big(\eta^2+\eta^2v^2+v\big)XY^4\\ &\qquad+\big(v\big(\eta^2+\eta^2u^2+u\big)+u(1+u+v)\big)X^3Y^2\\ &\qquad+\big(u\big(\eta^2+\eta^2v^2+v\big)+v(1+u+v)\big)X^2Y^3\\ &\quad=\begin{cases}X^4Y+XY^4 & \text{if } (u,v)=(1,1) \text{ or } (\eta,1) \text{ or } (1,\eta),\\ \eta^2(X^4Y+XY^4) & \text{if } (u,v)=(\eta^2,\eta^2).\end{cases}\end{aligned}$$

Therefore

$$\frac{F_{(a,b,c)}(X,Y,uX+vY)}{X^4Y+XY^4}=\begin{cases}a+b+c+1 & \text{if } (u,v)=(1,1),\\ a+b\eta+c+1 & \text{if } (u,v)=(\eta,1),\\ a+b+c\eta+1 & \text{if } (u,v)=(1,\eta),\\ a+b\eta^2+c\eta^2+\eta^2 & \text{if } (u,v)=(\eta^2,\eta^2).\end{cases}$$

To sum up, $C_{(a,b,c)}$ has no $\mathbb{F}_4$-linear components if and only if

$$\begin{cases}abc\neq 0,\\ a+b+c+1\neq 0,\\ \eta a+b+c+1\neq 0,\\ a+\eta b+c+1\neq 0,\\ a+b+\eta c+1\neq 0.\end{cases}\tag{9}$$

From the condition $abc\neq 0$, the possibilities of the solutions of (9) are at most 10 up to permutations of coordinates, which is the number of ways to choose three elements from $\{1,\eta,\eta^2\}$ allowing repetition. Screening those 10 candidates by other four conditions of (9), we have the four solutions. Those four curves are nonsingular by Corollary 2.2. □

Proof of Theorem 4.1. (Step I) In this step, we show that if $C\in\mathcal{C}_5(\mathbb{F}_4)$ has the properties (i) and (ii), then no three of the four points of $Z(C)$ are collinear. The argument is similar to the proof of Theorem 2.1. Let $Z(C)=\{Q_1,\dots,Q_4\}$. Suppose Q_1,Q_2,Q_3 are collinear. Let l_4 be the line passing through these three points.[3] Note that $Q_4\notin l_4$ by the condition (ii). Choose an $\mathbb{F}_4$-line $l_5\ni Q_4$ but $l_5\not\ni Q_1,Q_2,Q_3$, and put $P_0=l_4\cap l_5$. Let $l_1,\dots,l_5$ be the five $\mathbb{F}_4$-lines passing through P_0. Then

[3] Here we reset the notations l_1,l_2,l_3, which are not assigned particular lines in advance.

$l_i(\mathbb{F}_4) \subset C$ for $i = 1, 2, 3$, because $l_i \cap Z(C) = \emptyset$. Choose coordinates X, Y, Z as $P_0 = (0, 0, 1)$ and consider the equation $F(X, Y, Z) = \sum_{i=0}^{5} F_{5-i}(X, Y)Z^i$ of C, where $F_j(X, Y) \in \mathbb{F}_4[X, Y]$ is homogeneous of degree j. Put

$$l_i(\mathbb{F}_4) = \{(\alpha_i, \beta_i, \gamma) \mid \gamma \in \mathbb{F}_4\} \cup \{(0, 0, 1)\}.$$

Then $F(\alpha_i, \beta_i, \gamma) = 0$ for any $\gamma \in \mathbb{F}_4 = \{0, 1, \eta, \eta^2\}$ and for any $i \in \{1, 2, 3\}$, that is,

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & \eta & \eta^2 & \eta^3 \\ 1 & \eta^2 & \eta^4 & \eta^6 \end{pmatrix} \begin{pmatrix} F_5(\alpha_i, \beta_i) \\ F_4(\alpha_i, \beta_i) + F_1(\alpha_i, \beta_i) \\ F_3(\alpha_i, \beta_i) + F_0 \\ F_2(\alpha_i, \beta_i) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

for $i = 1, 2, 3$. So $F_2(X, Y) = 0$ as a polynomial. Therefore, for any $\gamma \in \mathbb{F}_4$,

$$F(\alpha_5, \beta_5, \gamma) = F_5(\alpha_5, \beta_5) + \big(F_4(\alpha_5, \beta_5) + F_1(\alpha_5, \beta_5)\big)\gamma + \big(F_3(\alpha_5, \beta_5) + F_0\big)\gamma^2,$$

which is a nontrivial polynomial in γ because it is nonzero for a γ that corresponds to Q_4. Hence $\#((l_5(\mathbb{F}_4) \setminus \{P_0\}) \cap C) \leqslant 2$, which is a contradiction because $(l_5(\mathbb{F}_4) \setminus \{P_0\}) \cap C = l_5(\mathbb{F}_4) \setminus \{P_0, Q_4\}$.

(Step II) The claim of this step is that C coincides with one of the four curves described in Proposition 4.6 after suitable choice of coordinates. Since no three of the four points of $Z(C)$ are collinear by Step I, we can choose coordinates as $Z(C) = \{(1, 1, 1), (\eta, 1, 1), (1, \eta, 1), (1, 1, \eta)\}$. Let $F(X, Y, Z) = 0$ be an equation of C in these coordinates. Since $(1, 0, 0), (0, 1, 0), (0, 0, 1) \in \mathbb{P}^2(\mathbb{F}_4) \setminus Z(C) = C(\mathbb{F}_4)$, each coefficient of X^5, Y^5 and Z^5 in F is 0. Hence we may put $F(X, Y, 0) = aX^4Y + a'XY^4 + bX^3Y^2 + b'X^2Y^3$. Since $(1, \lambda, 0) \in C$ for any $\lambda \in \mathbb{F}_4$, $(a + a')\lambda + b\lambda^2 + b'\lambda^3 = 0$ has four solutions in λ. So $a + a' = b = b' = 0$. Applying the same argument to $F(X, 0, Z)$ and $F(0, Y, Z)$, we have

$$F(X, Y, Z) = a\big(X^4Y + XY^4\big) + b\big(Y^4Z + YZ^4\big) + c\big(Z^4X + ZX^4\big) + XYZh(X, Y, Z),$$

where

$$h(X, Y, Z) = \alpha_1X^2 + \alpha_2Y^2 + \alpha_3Z^2 + \beta_1XY + \beta_2YZ + \beta_3ZX.$$

Since $(1, 1, \eta^2), (1, \eta^2, 1), (\eta^2, 1, 1) \in C$, three relations between coefficients of h

$$\alpha_1 + \alpha_2 + \alpha_3\eta + \beta_1 + \beta_2\eta^2 + \beta_3\eta^2 = 0, \tag{10}$$

$$\alpha_1 + \alpha_2\eta + \alpha_3 + \beta_1\eta^2 + \beta_2\eta^2 + \beta_3 = 0, \tag{11}$$

$$\alpha_1\eta + \alpha_2 + \alpha_3 + \beta_1\eta^2 + \beta_2 + \beta_3\eta^2 = 0 \tag{12}$$

hold, where one should not forget in computation that the first three terms of F are 0 for any $\mathbb{F}_4$-point. Compute $(10) + (11) + \eta^2 \times (12)$. Then we get $\alpha_1 = \eta^2\beta_2$. Similarly, we get $\alpha_2 = \eta^2\beta_3$ and $\alpha_3 = \eta^2\beta_1$. Moreover, since $(\eta^2, \eta, 1), (\eta, \eta^2, 1) \in C$, we have

$$\beta_1\eta + \beta_2\eta^2 + \beta_3 = 0,$$
$$\beta_1\eta + \beta_2 + \beta_3\eta^2 = 0.$$

Hence $\beta_1 = \beta_2 = \beta_3$. If this is 0, then $\alpha_1 = \alpha_2 = \alpha_3 = 0$, which easily leads us a contradiction. Put $\beta_1 = \beta_2 = \beta_3 = \lambda \in \mathbb{F}_4^\times$. After the linear transformation $X \mapsto \lambda X$, $Y \mapsto \lambda Y$, $Z \mapsto \lambda Z$, $F(X, Y, Z)$ changes to a polynomial of type $F_{(a,b,c)}(X, Y, Z)$ with possibly different (a, b, c) from the original.

(Step III) The claim is that the four curves

$$C_{(\eta,\eta,\eta)},\quad C_{(\eta,\eta^2,\eta^2)},\quad C_{(\eta^2,\eta,\eta^2)},\quad C_{(\eta^2,\eta^2,\eta)}$$

are projectively equivalent over $\mathbb{F}_4$ each other. Except $C_{(\eta,\eta,\eta)}$, this claim is obvious because it is enough to consider permutations of coordinates X, Y, Z.

Now we give a projective transformation by which $C_{(\eta,\eta^2,\eta^2)}$ goes to $C_{(\eta,\eta,\eta)}$. Consider the projective transformation

$$\sigma : \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} \mapsto \begin{pmatrix} \eta^2 & \eta & \eta \\ \eta & \eta^2 & \eta \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} X \\ Y \\ Z \end{pmatrix}.$$

Then we have

$$\eta\big(X^4Y + XY^4\big) + \eta^2\big(Y^4Z + YZ^4\big) + \eta^2\big(Z^4X + ZX^4\big) \mapsto \eta\big(X^4Y + XY^4\big)$$

by using Lemma 4.5. Moreover by straightforward computation, we have

$$XYZ \mapsto \big(X^2 + Y^2 + \eta^2Z^2 + XY + \eta YZ + \eta ZX\big)Z$$

and

$$\eta^2\big(X^2 + Y^2 + Z^2\big) + XY + YZ + ZX \mapsto \eta X^2 + \eta Y^2 + 0Z^2 + XY + \eta^2 YZ + \eta^2 ZX.$$

Hence, by little laborious computation, we have

$$\begin{aligned} &XYZ\big(\eta^2\big(X^2 + Y^2 + Z^2\big) + XY + YZ + ZX\big) \\ &\quad\mapsto \eta\big(Y^4Z + YZ^4\big) + \eta\big(Z^4X + ZX^4\big) + XYZ\big(\eta^2\big(X^2 + Y^2 + Z^2\big) + XY + YZ + ZX\big). \end{aligned}$$

Therefore $\sigma(C_{(\eta,\eta^2,\eta^2)}) = C_{(\eta,\eta,\eta)}$. □

Appendix A

The purpose of this appendix is to see that each of the two strict inequalities $M_q(d) > M_q^i(d)$ and $M_q^i(d) > M_q^s(d)$ can occur for some (q, d)'s.

Proposition A.1. *Suppose $q \geqslant 37$. Then $M_q(4) = 2q + 2 > M_q^i(4)$.*

First we construct a reducible curve C of degree 4 with $N_q(C) = 2q+2$. Choose an irreducible conic C_1 over $\mathbb{F}_q$ and two points $P_1, P_3 \in C_1(\mathbb{F}_{q^2}) \setminus C_1(\mathbb{F}_q)$ that are not conjugate over $\mathbb{F}_q$. Let $P_2 = P_1^{(q)}$ and $P_4 = P_3^{(q)}$, where $P^{(q)}$ denotes the image of P by the Frobenius map over $\mathbb{F}_q$. Since these four points $P_1, \ldots, P_4$ are on the conic C_1, no 3 of them are collinear. Since the cycle $P_1 + \cdots + P_4$ on $\mathbb{P}^2$ is defined over $\mathbb{F}_q$, the linear system $\mathcal{G}$ of conics in $\mathbb{P}^2$ passing through these four points is defined over $\mathbb{F}_q$ and of projective dimension 1. Therefore $\mathcal{G}$ contains $q + 1$ conics defined over $\mathbb{F}_q$. Among these $q + 1$ conics, only 3 conics are unions of two lines. Hence we can choose another irreducible conic C_2 over $\mathbb{F}_q$ such that $C_1 \cap C_2 = \{P_1, \ldots, P_4\}$. Let $C = C_1 \cup C_2$. Then $N_q(C) = 2q + 2$.

Secondly we show that $2q+2 > M_q^i(4)$ if $q \geqslant 37$. We need the Hasse–Weil bound for an irreducible curve which may have singularities; if $C \in \mathcal{C}_d^i(\mathbb{F}_q)$, then $N_q(C) \leqslant q + 1 + (d-1)(d-2)\sqrt{q}$ [4, Th. 9.57]. In our case, $M_q^i(4) \leqslant q + 1 + 6\sqrt{q}$, which is smaller than $2q + 2$ if $q \geqslant 37$.

Finally let $C \in \mathcal{C}_4(\mathbb{F}_q)$ such that $N_q(C) = M_q(4)$. Since $M_q(4) > M_q^i(4)$, C can't be irreducible. Then it is easy to see that C must be a union of two irreducible conics described in the first paragraph.

Proposition A.2. *Suppose $q \geqslant 4$. Let $d = (q^n - 1)/(q - 1)$. If $n \geqslant 3$, then $M_{q^n}^i(d) > M_{q^n}^s(d)$.*

Proof. We consider the curve C with an affine equation

$$y^{q^{n-1}} + y^{q^{n-2}} + \cdots + y + 1 = x^{q^{n-1}+q^{n-2}+\cdots+1},$$

which is analogous to the Hermitian curve. The curve has one point on the line at infinity, and this point is $\mathbb{F}_{q^n}$-rational. In the affine part,

$$C(\mathbb{F}_{q^n}) = \{(0,\beta) \mid \beta \in \mathbb{F}_{q^n},\ \mathrm{Tr}(\beta) = 0\} \cup \{(\alpha,\beta) \mid \alpha,\beta \in \mathbb{F}_{q^n},\ \mathrm{Tr}(\beta) = \mathrm{Nm}(\alpha)\},$$

where Tr and Nm are the trace map $\mathbb{F}_{q^n} \to \mathbb{F}_q$ and the norm map $\mathbb{F}_{q^n}^\times \to \mathbb{F}_q^\times$ respectively. Therefore $N_{q^n}(C) = q^{2n-1} + 1$. Hence $M_{q^n}^i(d) \geqslant q^{2n-1} + 1$. On the other hand, by Stöhr and Voloch [9] and Hefez and Voloch [2],

$$M_{q^n}^s(d) \leqslant \max\left\{\frac{1}{2}d(d + q^n - 1), d(q^n - d + 2)\right\}.$$

Since

$$N_{q^n}(C) - \frac{1}{2}d(d + q^n - 1) = q\left(q^{n-1} + \frac{q^n - 1}{\sqrt{2}(q-1)}\right)\left(q^{n-1} - \frac{q^n - 1}{\sqrt{2}(q-1)}\right) + 1$$

and

$$N_{q^n}(C) - d(q^n - d + 2) = \frac{1}{(q-1)^2}(q^{2n-1} - q^{n+1} - q^n + q^2),$$

we have

$$q^{2n-1} + 1 > \max\left\{\frac{1}{2}d(d + q^n - 1), d(q^n - d + 2)\right\}.$$

Therefore $M_{q^n}^i(d) > M_{q^n}^s(d)$. □

References

[1] G. van der Geer, M. van der Vlugt, Tables of curves with many points, http://www.science.uva.nl/~geer/.
[2] A. Hefez, J.F. Voloch, Frobenius nonclassical curves, Arch. Math. (Basel) 54 (1990) 263–273; Correction, Arch. Math. (Basel) 57 (1991) 416.
[3] J.W.P. Hirschfeld, Projective Geometries over Finite Fields, second edition, Oxford University Press, Oxford, 1998.
[4] J.W.P. Hirschfeld, G. Korchmáros, F. Torres, Algebraic Curves over a Finite Field, Princeton Univ. Press, Princeton, Oxford, 2008.
[5] M. Homma, S.J. Kim, Nonsingular plane filling curves of minimum degree over a finite field and their automorphism groups: Supplements to a work of Tallini, arXiv:0903.1918, 2009.
[6] M. Homma, S.J. Kim, Around Sziklai's conjecture on the number of points of a plane curve over a finite field, Finite Fields Appl. 15 (2009) 468–474.
[7] M. Homma, S.J. Kim, Sziklai's conjecture on the number of points of a plane curve over a finite field II, in: G. McGuire, G.L. Mullen, D. Panario, I.E. Shparlinski (Eds.), Finite Fields: Theory and Applications, in: Contemp. Math., vol. 518, Amer. Math. Soc., Providence, RI, 2010, pp. 225–234.

[8] M. Homma, S.J. Kim, Sziklai's conjecture on the number of points of a plane curve over a finite field III, Finite Fields Appl. 16 (2010) 315–319.
[9] K.-O. Stöhr, J.F. Voloch, Weierstrass points and curves over finite fields, Proc. Lond. Math. Soc. (3) 52 (1986) 1–19.
[10] J.-P. Serre, Rational points on curves over finite fields, Notes by Fernando Q. Gouvêa of lectures at Harvard University, 1985.
[11] P. Sziklai, A bound on the number of points of a plane curve, Finite Fields Appl. 14 (2008) 41–43.
[12] G. Tallini, Sulle ipersuperficie irriducibili d'ordine minimo che contengono tutti i punti di uno spazio di Galois $S_{r,q}$, Rend. Mat. Appl. (5) 20 (1961) 431–479.